

(translation)

JC825 U.S. PTO  
09/726564  
12/01/00

PATENT OFFICE  
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of  
the following application as filed with this office.

Date of Application: December 8, 1999

Application Number: Japanese Patent Application  
No. 11-348782

Applicant(s): Pioneer Corporation

Date of this certificate: August 11, 2000

Commissioner,  
Patent Office Kozo OIKAWA

Certificate No. 2000-3063063

日 本 国 特 許 庁  
PATENT OFFICE  
JAPANESE GOVERNMENT

JC625 U.S. PTO  
09/726564  
12/01/00

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application:

1 9 9 9 年 1 2 月 8 日

出 願 番 号  
Application Number:

平成 1 1 年 特 許 願 第 3 4 8 7 8 2 号

出 願 人  
Applicant (s):

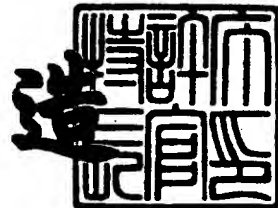
パイオニア株式会社

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2 0 0 0 年 8 月 1 1 日

特 許 庁 長 官  
Commissioner,  
Patent Office

及 川 耕 造



出 証 番 号 出 証 特 2 0 0 0 - 3 0 6 3 0 6 3

【書類名】 特許願  
【整理番号】 54P0379  
【提出日】 平成11年12月 8日  
【あて先】 特許庁長官殿  
【国際特許分類】 G11B 20/10  
G06F 7/00  
H04L 29/00

【発明者】

【住所又は居所】 埼玉県川越市大字山田字西町 2 5 番地 1 パイオニア株式会社川越工場内

【氏名】 野中 慶也

【発明者】

【住所又は居所】 東京都目黒区目黒 1 丁目 4 番 1 号 パイオニア株式会社内

【氏名】 柴崎 裕昭

【特許出願人】

【識別番号】 000005016

【氏名又は名称】 パイオニア株式会社

【代理人】

【識別番号】 100063565

【弁理士】

【氏名又は名称】 小橋 信淳

【手数料の表示】

【予納台帳番号】 011659

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

特平 1 1 - 3 4 8 7 8 2

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報記録読取方法ならびに装置

【特許請求の範囲】

【請求項 1】 それぞれに固有の識別情報が付された第一の記録媒体と第二の記録媒体とに対して、情報の記録または記録された情報の読取りを行う情報記録読取方法であって、

前記第一の記録媒体に付された識別情報に基づいて暗号化され記録された第一の暗号化情報を読取り、

前記読取られた第一の暗号化情報を、前記第二の記録媒体に付された識別情報に基づいて暗号化して第二の暗号化情報を生成し、

前記生成された第二の暗号化情報を前記第二の記録媒体に記録し、

前記第二の記録媒体から第二の暗号化情報を読み取り、前記第二の暗号化情報を前記第二の記録媒体が持つ識別情報に基づいて解読し、

前記解読された第二の暗号化情報を前記第一の暗号化情報として復元し前記第一の記録媒体に記録すること、  
を特徴とする情報記録読取方法。

【請求項 2】 前記第一、第二の記録媒体の認証を行い、いずれも正規の記録媒体と認証された場合に、前記第一、第二の記録媒体からそれぞれの暗号化情報の読取りを許可することを特徴とする請求項 1 に記載の情報記録読取方法。

【請求項 3】 第一の記録媒体が持つ識別情報に基づいて暗号化され記録された第一の暗号化情報を読みとり、当該第一の暗号化情報を第二の記録媒体に記録する情報記録読取装置であって、

前記第一の記録媒体から第一の暗号化情報を読取る読取手段と、

前記読取られた第一の暗号化情報を、前記第二の記録媒体が持つ識別情報に基づいて暗号化して第二の暗号化情報を生成する暗号化手段と、

前記生成された第二の暗号化情報を、前記第二の記録媒体に記録する記録手段と、

を有することを特徴とする情報記録読取装置。

【請求項 4】 前記読取手段は、

前記第一、第二の記録媒体の認証を行う認証手段と、

前記認証手段によって、前記第一、第二の記録媒体がいずれも正規の記録媒体と認証された場合、前記第一の暗号化情報の読取りを許可する許可手段と、  
を更に有することを特徴とする請求項 3 に記載の情報記録読取装置。

【請求項 5】 第二の記録媒体が持つ識別情報に基づいて暗号化された第二の暗号化情報を読み取り、当該第二の暗号化情報を第一の記録媒体に記録する情報記録読取装置であって、

前記第二の記録媒体から第二の暗号化情報を読取る読取手段と、

前記第二の暗号化情報を前記第二の記録媒体が持つ識別情報に基づいて解読する解読手段と、

前記解読された第二の暗号化情報を第一の暗号化情報として復元し前記第一の記録媒体に記録する記録手段と、

を有することを特徴とする情報記録読取装置。

【請求項 6】 前記読取手段は、更に、

前記第一、第二の記録媒体の認証を行う認証手段と、

前記認証手段によって、前記第一、第二の記録媒体がいずれも正規の記録媒体であると認証された場合、前記第二の暗号化情報の読取りを許可する許可手段と

を有することを特徴とする請求項 5 に記載の情報記録読取装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、音楽や映像、或いはコンピュータプログラム等の情報を記録再生する装置に用いて好適な、情報記録読取方法ならびに装置に関する。

【0002】

【従来の技術】

音楽や映像、或いはコンピュータプログラムなどの情報（著作物）を、通信によって電子的に配信する頒布方法が主流になりつつある。かかる頒布方法では、情報の正規の供給元からの頒布のみを認める取り決めが必要である。つまり、違

法なコピーが氾濫して、著作権者に多大な不利益を生じることが無いように、情報を受信してこれを記録、再生する装置において、一方の装置から他方の装置へのコピーを禁止する取り決めをしておかなければならない。ここでいうコピーとは、同時に２種類以上の媒体上に、同一のデータが存在している状態をいう。

【０００３】

【発明が解決しようとする課題】

しかしながら、上記の取り決めによると、バックアップするためのコピーであっても認められないことになり、正規にその著作物を入手したユーザに不利益を生じかねない。例えば、ＨＤＤ（ハードディスク）内に格納された音楽、映像、あるいはプログラムデータが何らかの原因により破壊された場合には再度入手する必要があり、場合によっては入手できなかったり、あるいはプログラムの場合、バージョンアップ等の関係により対応できないことも考えられる。

【０００４】

本発明は上記事情に鑑みてなされたものであり、複数の記録媒体を有する情報記録読取装置において、第一の記録媒体に記録された情報データを、バックアップ用の第二の記録媒体に記録する際、バックアップ用の第二の記録媒体に固有の識別情報に基づき暗号化して記録することにより第一の記録媒体とはその内容を異にし、このことにより、コピー禁止の概念を維持しつつ、バックアップするための記録を可能とする、情報記録読取方法ならびに装置を提供することを目的とする。

【０００５】

【課題を解決するための手段】

上記した課題を解決するために請求項１に記載の情報記録読取方法は、それぞれに固有の識別情報が付された第一の記録媒体と第二の記録媒体とに対して情報の記録または記録された情報の読取りを行う情報記録読取方法であって、前記第一の記憶媒体に付された識別情報に基づいて暗号化され記録された第一の暗号化情報を読取り、前記読取られた第一の暗号化情報を、前記第二の記録媒体に付された識別情報に基づいて暗号化して第二の暗号化情報を生成し、前記生成された第二の暗号化情報を前記第二の記録媒体に記録し、前記第二の記録媒体から第二

の暗号化情報を読み取り、前記第二の暗号化情報を前記第二の記録媒体が持つ識別情報に基づいて解読し、前記解読された第二の暗号化情報を前記第一の暗号化情報として復元し前記第一の記録媒体に記録することとした。

【0006】

また、請求項2に記載の情報記録読取方法は、請求項1に記載の同方法において、前記第一、第二の記録媒体の認証を行い、いずれも正規の記録媒体と認証された場合に前記第一、第二の記録媒体からそれぞれの暗号化情報の読取りを許可することとした。

【0007】

このことにより、第一の記録媒体に記録された情報を、バックアップ用の第二の記録媒体に記録する際、第二の記録媒体に固有の識別情報（第二の識別情報）に基づいて暗号化されて記録される。つまり、第二の記録媒体に記録される情報は、第二の識別情報に基づいて暗号化されたものであるから、第一の暗号化情報とは異なるものとなり、同一の情報を複製するというコピーの概念には当たらなくなる。従って、コピー禁止の概念を維持しつつ、バックアップするための記録が可能となる。また、バックアップにあたり相互認証を実行しながら行っているため不正なコピーの生成は発生しない。

【0008】

請求項3に記載の情報記録読取装置は、第一の記録媒体が持つ識別情報に基づいて暗号化され記録された第一の暗号化情報を読みとり、当該第一の暗号化情報を第二の記録媒体に記録する情報記録読取り装置であって、前記第一の記録媒体から第一の暗号化情報を読取る読取り手段と、前記読取られた第一の暗号化情報を、前記第二の記録媒体が持つ識別情報に基づいて暗号化して第二の暗号化情報を生成する暗号化手段と、前記生成された第二の暗号化情報を、前記第二の記録媒体に記録する記録手段とを有することとした。

【0009】

また、請求項4に記載の情報記録読取装置は、請求項3に記載の同装置において、前記読み取り手段は、更に、前記第一、第二の記録媒体の認証を行う認証手段と、前記認証手段によって、前記第一、第二の記録媒体がいずれも正規の記録



媒体と認証された場合、前記第一の暗号化情報の読取りを許可する許可手段とを有することとした。

【 0 0 1 0 】

請求項 5 に記載の情報記録読取装置は、第二の記録媒体が持つ識別情報に基づいて暗号化された第二の暗号化情報を読み取り、当該第二の暗号化情報を第一の記録媒体に記録する情報記録読取装置であって、前記第二の記録媒体から第二の暗号化情報を読取る読取手段と、前記第二の暗号化情報を前記第二の記録媒体が持つ識別情報に基づいて解読する解読手段と、前記解読された第二の暗号化情報を第一の暗号化情報として復元し前記第一の記録媒体に記録する記録手段とを有することとした。

【 0 0 1 1 】

また、請求項 6 に記載の情報記録読取装置は、請求項 5 に記載の同装置において、前記読取手段は、更に、前記第一、第二の記録媒体の認証を行う認証手段と、前記認証手段によって、前記第一、第二の記録媒体がいずれも正規の記録媒体であると認証された場合、前記第二の暗号化情報の読取りを許可する許可手段とを有することとした。

【 0 0 1 2 】

上記構成により、第一の記録媒体に記録された内容を第二の記録媒体にバックアップする場合暗号化手段を介して暗号化される。ここでの暗号化は、第二の記録媒体に固有の識別情報（ID）を抽出し、かかる抽出した識別情報を暗号化するための鍵データとして用いることにより行われる。従って、ここでは、第一の記録媒体が持つ固有の識別情報で暗号化された情報は、更に第二の記録媒体が持つ識別情報で暗号化されることになる。一方、第一の記録媒体に記録されたデータ（元データ）が何らの原因によって破壊された場合には第二の記録媒体から得られるデータ（バックアップデータ）を用いて復元する必要がある。このとき、第二の記録媒体から読み出されたデータは復調され、解読手段によって第二の記録媒体が持つ識別情報を元に解読が行われ、その解読された情報、つまり、第一の記録媒体が持つ固有の識別情報で暗号化された情報が第一の記録媒体に書き込まれる。このことにより、第一の記録媒体が持つ識別情報のみによって暗号化さ

れた情報が第一の記録媒体に書込まれたことになる。

【0013】

以上によりコピー禁止の概念を維持しつつ、バックアップするための記録、あるいは復元するための読取りが可能となる。尚、上記読取り及び書込みはいずれも相互認証を行うことによってなされるため、不正なコピーやデータが消失することはない。

【0014】

【発明の実施の形態】

図1は、本発明が採用される情報再生システムの実施形態を示す図である。情報再生システムは、音源となるホームサーバ1を核に、マンマシンインタフェースとなるワイヤレススピーカ3が複数分散配置されることによってユーザに再生情報が享受される構成になっている。そして、ユーザが携帯するワイヤレス端末2の移動に伴い、ホームサーバ1に接続されるワイヤレススピーカ3が選択されるようになっている。

【0015】

図2は、図1に示すホームサーバ1の内部構成を示すブロック図である。図において、11は親機となる当該ホームサーバ1の制御中枢となるCPUである。CPU11は、操作キー12を介してユーザから与えられる指令を解読して表示部13に処理結果を表示したり、後述する各ブロックの制御を行う。CPU11は、上記したいずれの制御も内蔵プログラム（図示せず）を読み出し逐次実行することによりなされる。14はIDROMであり、当該ホームサーバ1が持つユニークな識別番号を主に格納するメモリである。

【0016】

15は送受信ユニットであり、制御部151を核に、送信部152と受信部153で構成される。送信部152は、CPU11ならびに制御部151による制御の下、CDプレーヤ45、チューナ46、HDD16等の音源からアドレスデータバス161、162経由で供給される音声信号を、マルチプレクサ17、エンコーダ18を介して変調し、マンマシンインタフェースとなる複数のワイヤレススピーカ3へ送信する。受信部153は、CPU11ならびに制御部151に

よる制御の下、ワイヤレス端末 2、またはワイヤレススピーカ 3 から供給される信号を受信し、デコーダ 1 9 で復元し、必要に応じてデマルチプレクサ 2 0、アドレスデータバス 1 6 1、1 6 2 経由で HDD 1 6 にダウンロードする。

【0 0 1 7】

4 4 はバックアップ用 HDD であり、HDD 1 6 と同じくアドレスデータバス 1 6 1、1 6 2 に接続され、CPU 1 1 による制御の下で音楽データが記録され、また、読出され、音源として再生系に供給するものとする。図 5 にその詳細が示されている。

【0 0 1 8】

図 3 は、図 1 に示すワイヤレス端末 2 の内部構成を示すブロック図である。図において、2 1 は子機となる当該ワイヤレス端末 2 の制御中枢となる CPU である。CPU 2 1 は、命令コード記憶部 2 5 に格納された再生指令や記録指令等を表す命令コード（後述するリレーコードを含む）を読出し実行する他、操作キー 2 2、表示部 2 3 による入出力処理を行う。2 4 は IDROM であり、主に当該ワイヤレス端末のユニークな識別番号（ID）が格納されている。

【0 0 1 9】

2 6 は送受信ユニットであり、制御部 2 6 1 を核に、送信部 2 6 2 と受信部 2 6 3 で構成される。送信部 2 6 2 は、CPU 2 1 ならびに制御部 2 6 1 による制御の下、エンコーダ 4 2 を介して変調された信号をホームサーバ 1 及びワイヤレススピーカ 3 に供給する。受信部 2 6 3 は、CPU 2 1 及び制御部 2 6 1 による制御の下、受信した信号をデコーダ 4 1 によって復元し、デマルチプレクサ 4 3 を介して CPU 2 1 に供給する。HDD 2 7 に記録された音声情報は、CPU 2 1 による制御の下、D/A 変換器 2 8 を介してアナログ信号に変換され、アンプ 2 9 経由でワイヤレス端末 2 が持つ携帯スピーカ 3 0 に供給される。

【0 0 2 0】

図 4 は、図 1 に示すワイヤレススピーカ 3 の内部構成を示すブロック図である。図において、3 1 は子機となる当該ワイヤレススピーカ 3 の制御中枢となる CPU である。CPU 3 1 は、内蔵するプログラムに従い後述する各ブロックの制御を行う。3 2 は IDROM であり、当該ワイヤレススピーカ 3 に付されたユニ

ークな識別番号が主に格納されるメモリである。

#### 【 0 0 2 1 】

3 3 は送受信ユニットであり、制御部 3 3 1 を核に、送信部 3 3 2、受信部 3 3 3、そして、電界強度測定部 3 3 4 で構成される。送信部 3 3 2 は、CPU 3 1 により生成される信号をエンコーダ 3 6 を介して変調し、親機であるホームサーバ 1 あるいは子機であるワイヤレス端末 2 へ供給する。受信部 3 3 3 は、制御部 3 3 1 による制御の下、親機であるホームサーバ 1 から受信した音声信号をデコーダ 3 7 により復元し、デマルチプレクサ 3 8 経由で CPU 3 1 に供給する。CPU 3 1 が受信した音声信号は、D/A 変換器 3 9 を介してアナログ信号に変換され、アンプ 3 4 経由でマンマシンインタフェースとしてのスピーカ 3 5 に供給され所望の音声として出力される。

#### 【 0 0 2 2 】

尚、電界強度測定部 3 3 4 は、CPU 3 1 による制御の下、子機であるワイヤレス端末 2 から発せられるリレーコードの電界強度を測定する部分であり、ユーザが当該ワイヤレススピーカ 3 近傍（例えば半径 5 0 c m 四方）にいるか否かの判定のために微弱電力で発信されるリレーコードが使用される。リレーコードの受信結果は CPU 3 1 に供給される。

#### 【 0 0 2 3 】

上述した情報再生システムにおいて、本発明の情報記録読取装置は、例えばホームサーバ 1 に適用される。ホームサーバ 1 は、それぞれ固有の識別情報（ID）が付された元データを記録する元ディスクである HDD 1 6 と、バックアップデータを記録するバックアップ用ディスクである HDD 4 4 とを備え、元ディスクである一方の HDD 1 6 に付された媒体 ID（ID 1）に基づいて、例えば、DES（Data Encryption Standard）等の良く知られた暗号化技術を用いて暗号化され、記録された暗号化情報を読取り、ここで読取られた暗号化情報を更にバックアップ用の HDD 4 4 に付された媒体 ID（ID 2）に基づいて暗号化することによりバックアップ用データを生成し、この生成された暗号化情報をバックアップ用 HDD 4 4 に記録する。一方、HDD 1 6 に記録されている元データが何らかの理由により破壊された場合には、その媒体 ID（ID 2）を使用して

バックアップ用HDD 4 4 から元データを復元する。

【0 0 2 4】

尚、記録媒体に固有の識別情報であるIDは、本発明実施形態で用いられるHDDであればディスクの固定領域（FAT:File Allocation Table）に、また、光ディスクであればプリフォーマットとして同じく固定領域に書替え不可の状態を設定されている。本発明では、これら記録媒体が物理的に破壊されない限り、IDが書き替えられることはないことを前提に以下に詳細に説明する。

【0 0 2 5】

図5は、図1に示すホームサーバ1のHDD 1 6、4 4 が持つ周辺回路の詳細を示すブロック図である。図中、Aサイドに元ディスクとなるHDD 1 6の周辺回路が、BサイドにバックアップディスクとなるHDD 4 4の周辺回路が示されている。

【0 0 2 6】

HDD 1 6の周辺回路は、ピックアップユニット1 1 1、復調器1 1 2、変調器1 1 3、解読器1 1 4、1 1 8、ID抽出回路1 1 5、ドライブCPU 1 1 6、マルチプレクサ1 1 7、暗号器1 1 9で構成される。HDD 4 4の周辺回路は、ピックアップユニット1 2 0、変調器1 2 1、復調器1 2 2、暗号器1 2 3、ドライブCPU 1 2 4、ID抽出回路1 2 5で構成される。

【0 0 2 7】

HDD 1 6の周辺回路にあるピックアップユニット1 1 1は、元ディスク1 6に対してリードライトを行うために用意される磁気ヘッドを含むリードライト回路である。ここで書き込まれる内容は、例えば、外部から通信により供給される入力データを、暗号器1 1 9により元ディスク1 6が持つ媒体IDに従って暗号化することにより生成される。ここでの暗号化は、ID抽出回路1 1 5によって抽出されたID 1 がドライブCPU 1 1 6経由で供給されることによりなされる。そして、マルチプレクサ1 1 7、変調器1 1 3経由でピックアップ1 1 1に供給し、元ディスク1 6に書込む。また、元ディスク1 6から読出されたデータは、復調器1 1 2を経由し、解読器1 1 4で暗号化が解かれて、ホームサーバ1が持つD/A変換回路等の再生系（図示せず）に出力される。

## 【0028】

一方、元ディスク16に記録された内容をHDD44にバックアップする場合は、元ディスク16からピックアップ111、復調器112経由で読出された内容は、Bサイドに示されるHDD44周辺回路にある暗号器123で暗号化される。ここでの暗号化は、ドライブCPU124の制御の下でID抽出回路125によって抽出されるバックアップ用HDD44の媒体ID（ID2）がドライブCPU124を経由して供給され、このIDに基づいて暗号化される。従って、ここでは、ID1で暗号化された情報が更にID2で暗号化されることになる。

## 【0029】

元ディスク16に記録されていたデータが何らの原因により破壊された場合には、バックアップディスク44から得られるデータを復元する。このき、バックアップディスク44からピックアップ120経由で読み出されたデータは、復調器122によって復調され、ドライブCPU124の制御の下、HDD16の周辺回路の解読器118に供給される。解読器118では、復調器122から得られるデータに関し、ドライブCPU116を介して通知されるバックアップ用HDD44の媒体IDであるID2による暗号化を解いて、ID2を分離してマルチプレクサ117、変調器113経由でピックアップ111へ供給する。このことにより、ピックアップユニット111は、ID1のみにより暗号化された情報を元ディスク16に書き込む。

## 【0030】

尚、上述した各ブロックは、いずれもハードウェアとして説明したが、一部をドライブCPU116、124が持つファームウェアで実現してもよい。

## 【0031】

図6、図7は本発明実施形態の動作を示すフローチャートであり、それぞれ、バックアップ記録の際におけるドライブCPU124の動作手順、復元記録の際におけるドライブCPU116の動作手順が示されている。いずれも（a）はメインルーチン、（b）あるいは（c）はサブルーチンを示す。

## 【0032】

以下、図6、図7を参照しながら図5に示す本発明実施形態の動作について詳

細に説明する。まず、ドライブCPU124は、ドライブCPU116との間で相互認証処理を行う（ステップS61）。相互認証は、図6（b）に示すように、CPU116に対してあらかじめ定義された認証コードを要求し（ステップS611）、その認証コードをチェックして（ステップS611）、それが所定のコードであれば、あらかじめ定義されたドライブCPU124の認証コードをドライブCPU116に送出し（ステップS613）、ドライブCPU116からACKが返答されたときに認証成功（ステップS614）とする。認証が失敗に終わった場合はエラーとする（ステップS615）。

#### 【0033】

次に、ドライブCPU124は、バックアップディスク44の媒体ID（ID2）を抽出する（ステップS62）。そしてドライブCPU116に対してデータ転送要求を発行し（ステップS63）、元ディスク16から元データを供給することを要求し、そのデータに基づいて記録処理を行う（ステップS64）。記録処理は、図6（c）に示すように、暗号器123でドライブCPU124を介して供給されるID2に基づき、復調器112から得られる元データ（ID1により暗号化済み）を暗号化し（ステップS641）、変調器121で記録変調して、ピックアップ120経由でバックアップディスク44にその内容を書き込む（ステップS642）ことによりなされる。そして、所望の所定量のデータ転送が終了したか否かをチェック（ステップS65）し、否の場合、ステップS63以降の処理を繰り返し全ての転送終了を待ってバックアップ処理を終える。

#### 【0034】

次に、元データが何らかの原因により破壊されたときのバックアップディスク44による復元記録処理について図7のフローチャートを参照しながら説明する。まず、ドライブCPU116は、相互認証処理を行う（ステップS71）。相互認証処理は、図6（b）で示す手順と同様である。次に、ドライブCPU124に対してバックアップディスク44の媒体IDであるID2の送信要求を発行する（ステップS72）。そして、バックアップディスク44からのデータ転送を要求し（ステップS73）、元ディスク16への記録処理を実行する（ステップS74）。

## 【 0 0 3 5 】

記録処理は、図 7 (b) に示すように、ドライブ CPU 1 1 6 は、復調器 1 2 2 を介して得られるバックアップ用 HDD 4 4 の媒体 ID (ID 2) で暗号化されているバックアップデータを解読器 1 1 8 により、ステップ S 7 2 で供給された ID 2 に基づいて解読し (ステップ S 7 4 1)、マルチプレクサ 1 1 7 を介して変調器 1 1 3 で記録変調する (ステップ S 7 4 2)。変調器 1 1 3 で記録変調されたバックアップデータは、ピックアップユニット 1 1 1 経由で元ディスク 1 6 に書き込まれる。

## 【 0 0 3 6 】

次に、所望の所定量のデータ転送が終了したか否かをチェック (ステップ S 7 5) し、否の場合、ステップ S 7 3 以降の処理を繰り返し全ての転送終了を待つて復元記録処理を終える。

## 【 0 0 3 7 】

以上説明のように本発明は、第一の記録媒体 1 6 に記録された元データをバックアップするとき、第一の記憶媒体に付された識別情報 (ID 1) に基づいて暗号化され記録される第一の暗号化情報を読み取り、読取られた第一の暗号化情報を、バックアップ用の第二の記録媒体 4 4 に付された識別情報 (ID 2) に基づいて暗号化して第二の暗号化情報を生成し、ここで生成された第二の暗号化情報を第二の記録媒体に記録する。バックアップデータを復元するとき、第二の記録媒体から第二の暗号化情報を読み取り、第二の暗号化情報を第二の記録媒体が持つ識別情報に基づいて解読し、この解読された第二の暗号化情報を第一の暗号化情報として復元して第一の記録媒体に記録するものである。このことによりバックアップ記録が可能となり、正規のユーザに不利益を与えることなく、著作権者の権利を保護することができる。

## 【 0 0 3 8 】

## 【発明の効果】

以上説明のように本発明によれば、複数の記録媒体を有する情報記録読取り装置において、第一の記録媒体に記録された情報データを、バックアップ用の第二の記録媒体に記録する際、バックアップ用の第二の記録媒体に固有の識別情報に



に基づき暗号化して記録することにより、第一の記録媒体とはその内容を異にし、このことにより、コピー禁止の概念を維持しつつ、バックアップするための記録を可能とするものである。また、何らかの原因により第一の記録媒体に記録された元データが破壊されたとき、第二の記録媒体が持つ識別情報に基づき解読することによって第一の記録媒体に元データの復元が可能となる。更に、上記した記録、復元は相互認証により行われるため、違法なコピーを防止できる。

【0039】

従って、著作権者に対する権利の保護がはかれると共に、更に、正規のユーザにも不利益が生じることが無いようにコピー禁止の概念を維持しつつバックアップのための記録が可能となり、今後の情報通信分野において有効な手段となる。

【図面の簡単な説明】

【図1】 本発明が採用される情報再生システムの構成例を示すブロック図である。

【図2】 図1におけるホームサーバの内部構成を示すブロック図である。

【図3】 図1におけるワイヤレス端末の内部構成を示すブロック図である。

【図4】 図1におけるワイヤレススピーカの内部構成を示すブロック図である。

【図5】 図1、図2に示すホームサーバのうち、本発明と関係する部分のみ抽出して示したブロック図である。

【図6】 本発明実施形態の動作手順をフローチャートで示した図である。

【図7】 本発明実施形態の動作手順をフローチャートで示した図である。

【符号の説明】

1…ホームサーバ、2…ワイヤレス端末、11(21、31)…CPU、12(22)…操作キー、14(24、32)…IDROM、15(26、33)…送受信ユニット、16(27)…ハードディスク装置(HDD)、44…バックアップディスク装置(HDD)、112(122)…復調器、113(121)…変調器、114(118)…解読器、115(125)…ID抽出回路、116(124)…ドライブCPU、117…マルチプレクサ、119(123)…

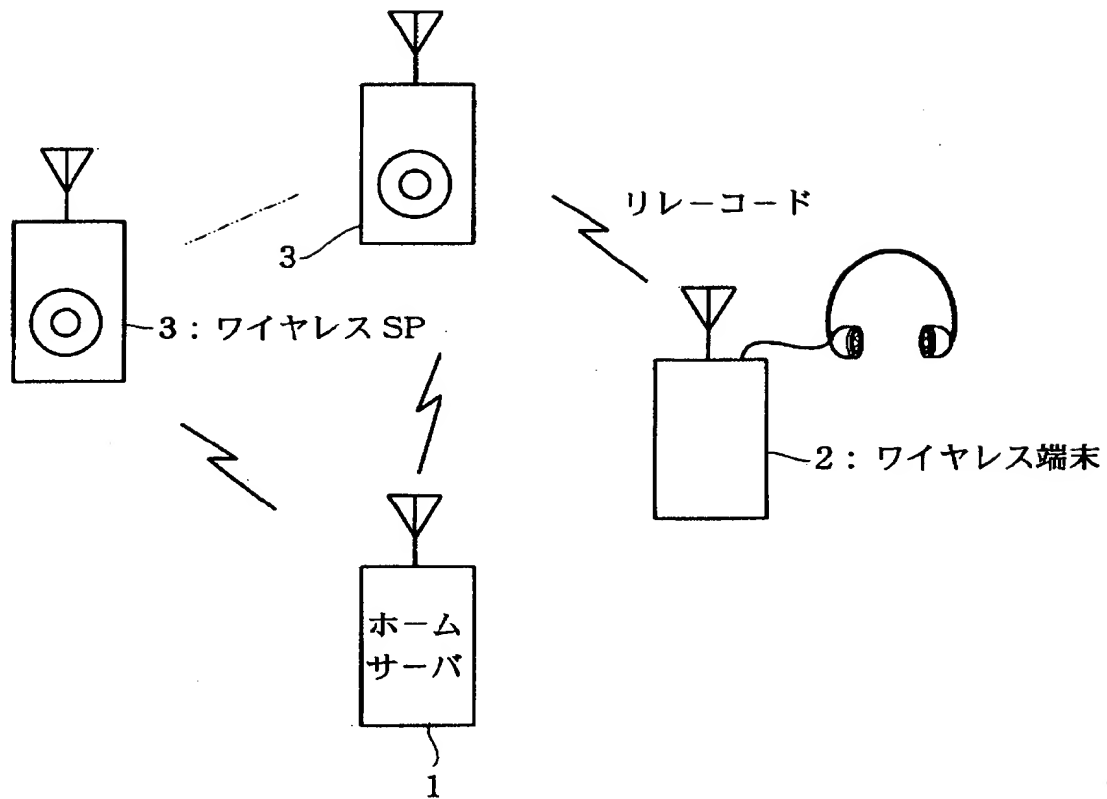
特平 1 1 - 3 4 8 7 8 2

暗号器

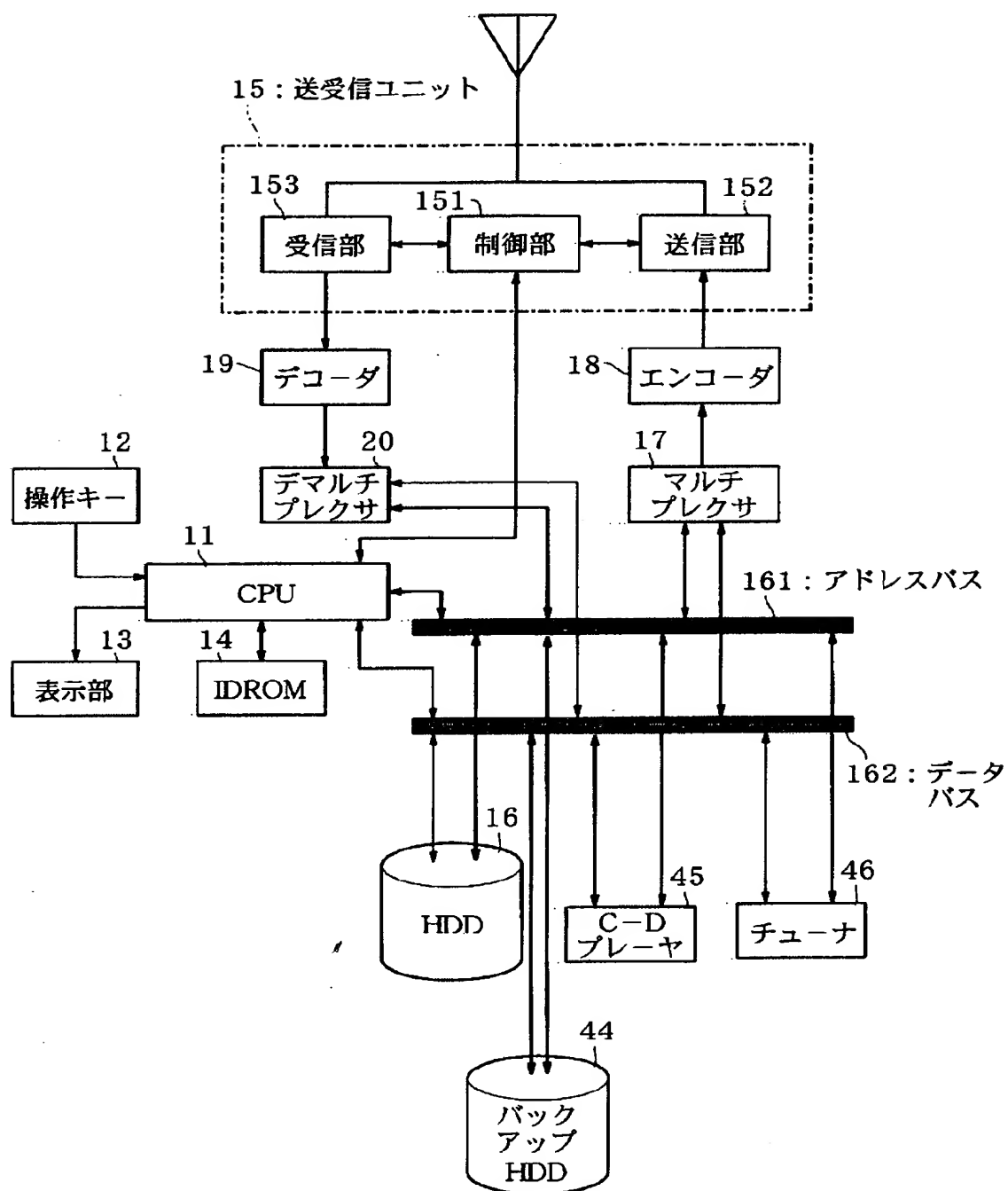
【書類名】

図面

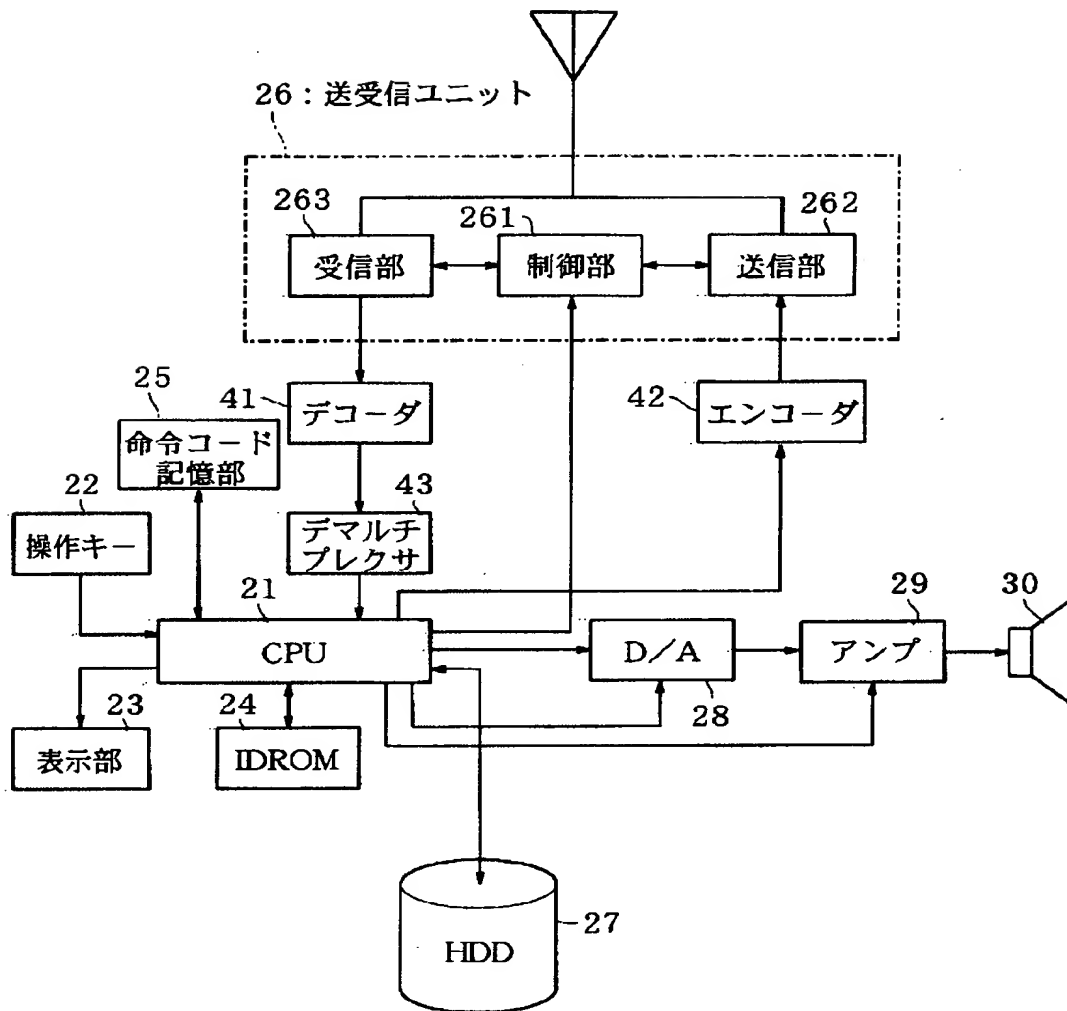
【図 1】



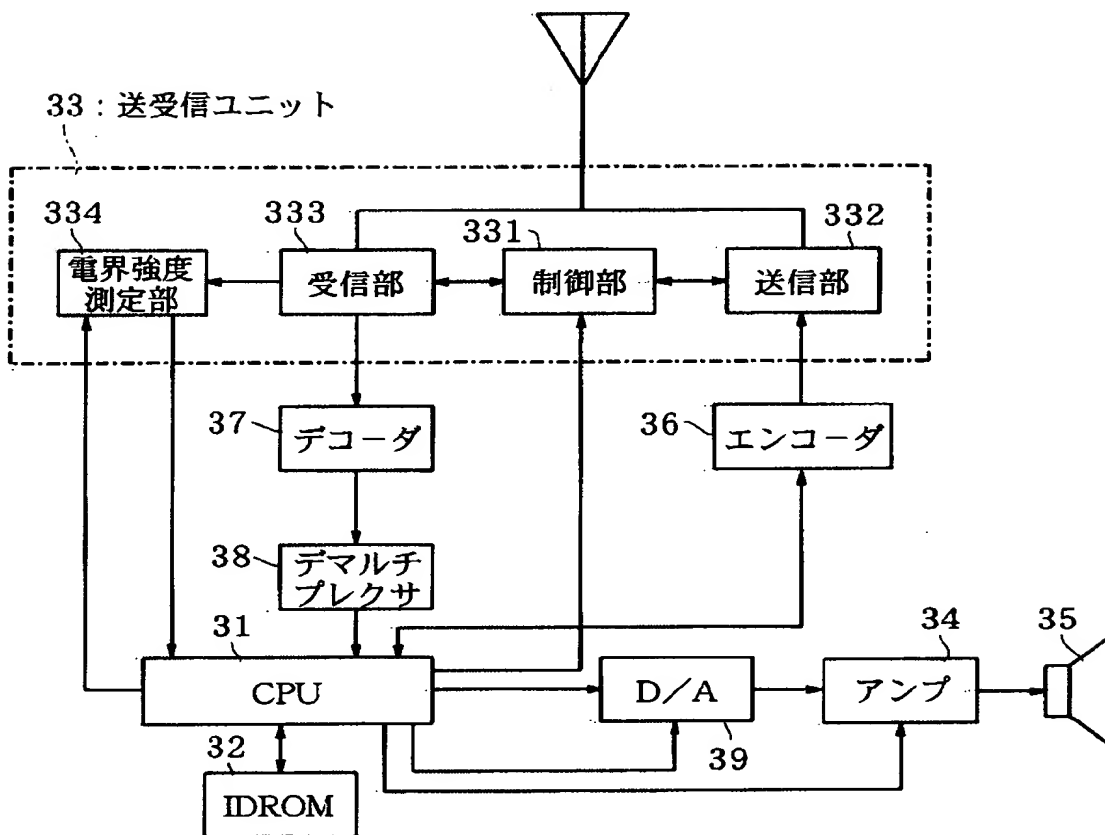
【図 2】



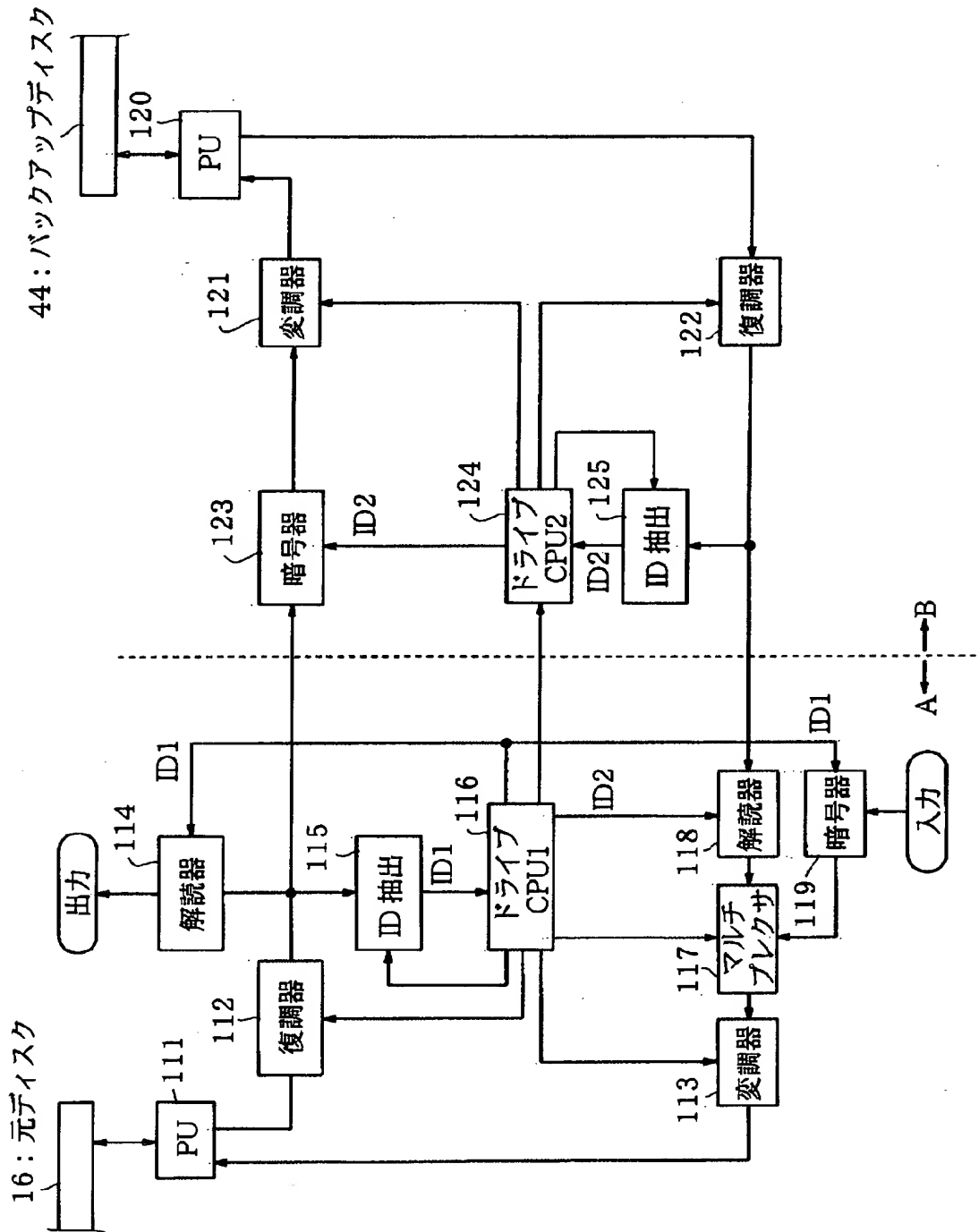
【図 3】



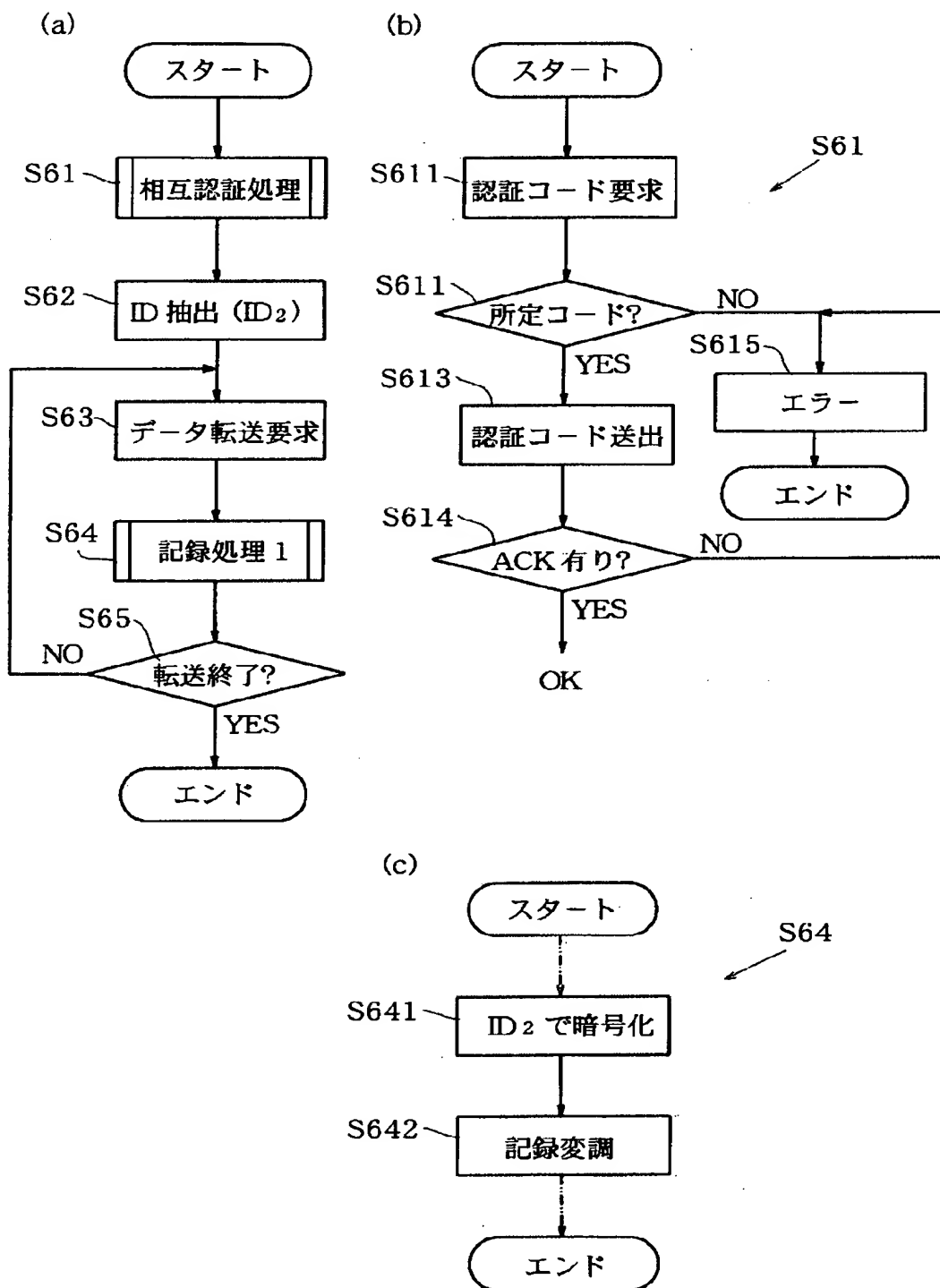
【図 4】



【図 5】

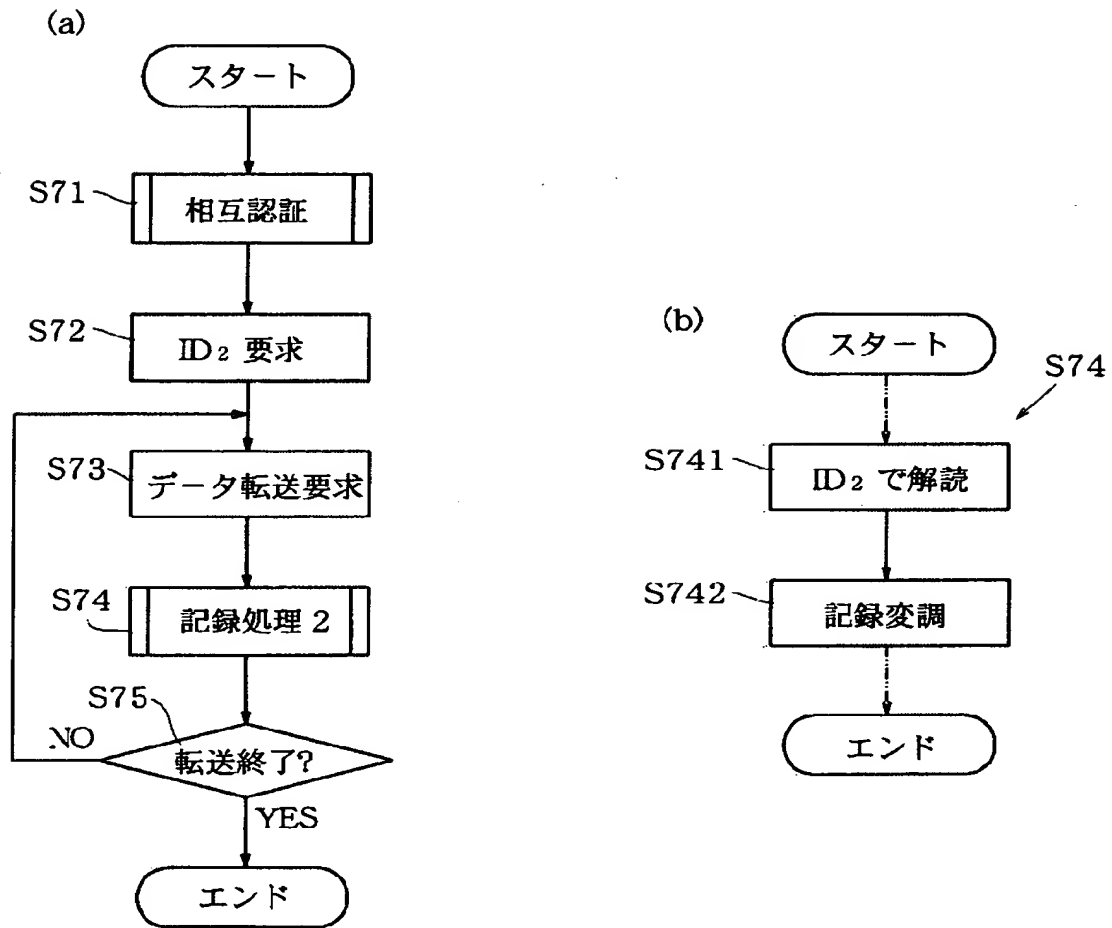


【図 6】





【図 7】



【書類名】 要約書

【要約】

【課題】 コピー禁止の概念を維持しつつ、データバックアップのための記録を可能とする。

【解決手段】 第一の記録媒体 1 6 に記録された元データをバックアップするとき、第一の記憶媒体に付された識別情報（I D 1）に基づいて暗号化され記録される第一の暗号化情報を読み取り、読み取られた第一の暗号化情報を、バックアップ用の第二の記録媒体 4 4 に付された識別情報（I D 2）に基づいて暗号化して第二の暗号化情報を生成し、ここで生成された第二の暗号化情報を第二の記録媒体に記録する。バックアップデータを復元するとき、第二の記録媒体から第二の暗号化情報を読み取り、第二の暗号化情報を第二の記録媒体が持つ識別情報に基づいて解読し、この解読された第二の暗号化情報を第一の暗号化情報として復元して第一の記録媒体に記録する。

【選択図】 図 2

出 願 人 履 歴 情 報

識別番号 [000005016]

1. 変更年月日	1990年 8月31日
[変更理由]	新規登録
住 所	東京都目黒区目黒1丁目4番1号
氏 名	パイオニア株式会社